# US-CERT Cyber Security Bulletin

***SB04-161*** ***June 9, 2004***

Information previously published in CyberNotes has been incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

## *Bugs, Holes & Patches*

The following tables provide a summary of software vulnerabilities identified between May 18 and June 8, 2004. The tables provides the risk, vendor and software name, potential vulnerability/impact, any identified patches/workarounds/alerts and whether attacks have utilized this vulnerability or an exploit script is known to exist and the common name/CVE number. Software versions and operating systems are identified if known. The tables are organized by operating system with new information identified first followed by updated information. ***Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.*** This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site. Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures. *Note: All the information included in the following tables has been discussed in newsgroups and websites.*

### *Windows Operating Systems*

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | craftysyntax.com[1]<br>Crafty Syntax Live Help 2.7.3 | A Cross-Site Script vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code.<br>Upgrade available at: http://prdownloads.sourceforge.net/cslive/CSLHv2.7.4.tar.gz?download<br>There is not exploit code required. | Crafty Syntax Live Help Multiple HTML Injection |

[1] Bugtraq, June 3, 2004.

| Risk* | Vendor & Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | e107.org[2]<br>e107 website system 0.6 10 -0.6 15a, 0.545, 0.554, 0.555 Beta, 0.603 | A Cross-Site Scripting vulnerability exists because 'usersettings.php' does not filter HTML code from user-supplied input before 'user.php' displays the information, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | e107 'usersettings.php' Cross-Site Scripting |
| High | Gallery Project[3]<br>Debian[4]<br>Debian Linux 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;<br>Gallery Gallery 1.4 -pl1-pl2, 1.4-1.4.3 -pl1 | A vulnerability exists due to an authentication error, which could let a remote malicious user obtain administrative access.<br>Upgrades available at:<br>http://prdownloads.sourceforge.net/gallery/gallery-1.4.3-pl2.tar.gz?download<br>**Debian:**<br>http://security.debian.org/pool/updates/main/g/gallery/<br>There is not exploit code required. | Gallery 'init.php' Authentication Flaw |
| High | Gregg Kenneth Jewell[5]<br>Mail Manage EX 3.1.8 | A vulnerability exists in the 'mmex.php' script due to insufficient validation of user-supplied input in the '$Settings' variable, which could let a remote malicious user execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Mail Manage EX Arbitrary File Inclusion |
| High | ldu.neocrome.net[6]<br>Land Down Under 700-01-03, 602, 601 | A Cross-Site Scripting vulnerability exists due to missing input validation of BBcode tags, which could let a remote malicious user execute arbitrary HTML and script code.<br>Upgrades available at:<br>http://ldu.neocrome.net/page.php?id=1357<br>A Proof of Concept exploit has been published. | Land Down Under BBCode Cross-Site Scripting |
| High | Microsoft[7]<br>Internet Explorer 6.0, SP1, | A vulnerability exists because it is possible to pass a dynamically created Iframe to a modal dialog, which could let a remote malicious user execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>A Proof of Concept exploit has been published. Exploits are also circulating in the wild. | Internet Explorer Modal Dialog Zone Bypass |
| High | Mollensoft Software[8]<br>Lightweight FTP Server 3.6 | A buffer overflow vulnerability exists due to insufficient boundary checks performed on CD command arguments, which could let a remote malicious user execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>A Proof of Concept exploit script has been published. | Lightweight FTP Server Remote Buffer Overflow |

[2] R.A.M Security Advisory, May 22, 2004.
[3] Gallery Security Release, June 1, 2004.
[4] Debian Security Advisory, DSA 512-1, June 2, 2004.
[5] Secunia Advisory, SA11774, June 3, 2004.
[6] Securiteam, May 30, 2004.
[7] Bugtraq, June 7, 2004.

| Risk* | Vendor & Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | Oracle Corporation[9]<br><br>Oracle Applications 11.0, E-Business Suite 11.0, E-Business Suite 11i 11.5.1-11.5.8 | Multiple vulnerabilities exist due to input validation errors, which could let a remote malicious user execute arbitrary code.<br><br>Patches available at:<br>http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=274375.1<br><br>There is not exploit code required. | Oracle E-Business Suite Multiple Input Validation |
| High | Pawel Jaczewski[10]<br><br>JPortal Web Portal 2.2.1 | An input validation vulnerability exists in 'module/print.inc.php' due to insufficient filtering of user-supplied data, which could let a remote malicious user execute arbitrary SQL commands.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | JPortal 'Print.php' SQL Injection |
| High | PHP Group[11]<br>Apple<br>Caldera<br>Conectiva<br>Debian<br>Engarde<br>FreeBSD<br>Gentoo<br>HP<br>IBM<br>Mandrake<br>OpenPKG<br>RedHat<br>Slackware<br>Sun Microsystems<br>SuSE<br>Trustix<br><br>PHP 3.0, 3.0 .13-3.0 .18, 3.0.1-3.0.13, 3.0.16, 4.0, 4.0.1 pl1&pl2, 4.0.1-4.0.7, RC1-RC3, 4.1.0-4.1.2, 4.2 .0, 4.2 –dev, 4.2.1-4.2.3, 4.3-4.3.3, 4.3.6, 5.0 candidate 1 & 2 | A vulnerability exists in the PHP 'include()' function when an application uses a user-supplied URI parameter as an argument, which could let a remote malicious user execute arbitrary commands.<br><br>No workaround or patch available at time of publishing.<br><br>Exploit script has been published. | PHP 'include()' function Remote Command Execution |

[8] EOS Advisory, May 28, 2004.
[9] Oracle Security Alert 67, June 3, 2004.
[10] Secunia Advisory, SA11737, May 31, 2004.
[11] Bugtraq, May 27, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | Real Networks[12]<br><br>RealPlayer G2, 6.0 Win32, 6.0 Unix, 7.0 Win32, 7.0 Unix, 7.0 Mac, 8.0 Win32, 8.0 Unix. 8.0 Mac, 10.0 BETA, 10.0 v6.0.12.690, RealPlayer for Windows 7.0 | A vulnerability exists in the default installations of RealPlayer, which could let a remote malicious user execute arbitrary code.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required. | RealNetworks RealPlayer Remote Code Execution |
| High | Riverdeep Interactive Learning[13]<br><br>SmartStuff FoolProof Security 3.9.4, 3.9.7 | A vulnerability exists because the password recovery algorithm can be manipulated to recover an 'Administrator' password, which could let a malicious user obtain administrative access.<br><br>No workaround or patch available at time of publishing.<br><br>Exploit script has been published. | FoolProof Security Program Administrative Password Recovery |

[12] SecurityTracker Alert, 1010396, June 4, 2004.
[13] SecurityFocus, June 5, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | Trend Micro[14]<br><br>InterScan VirusWall 3.0.1, 3.2.3, 3.3, 3.6, Build 1166, Build 1182, 3.7, Build 1190, 3.8 Build 1130, 3.32, 3.52, (HP-UX) 3.6, (Linux) 3.0.1, (Linux) 3.6, (Solaris) 3.6 Unix 3.0.1, 3.6 x, Windows NT 3.4, 3.5, 3.6, 3.51, 3.52, build 1466, 5.1, InterScan WebManager 1.2, 2.0, 2.1, OfficeScan Corporate Edition 3.0, 3.5, 3.11, 3.13, 3.54, 5.02, 5.58, OfficeScan Corporate Edition for Windows NT Server 3.0, 3.1.1, 3.5, 3.11, 3.13, OfficeScan For Microsoft SBS 4.5, Micro PC-cillin 2003, 2002, 2000, 6.0, ScanMail 1.0, ScanMail for Microsoft Exchange 3.8, 3.81, 6.1, Scanning Engine 7.1, Virus Buster Corporate Edition 3.52-3.54, Virusbuster 2001 8.0.1, 8.0.2, Viruswall 3.0.1 | A vulnerability exists due to insufficient sanitization of user-supplied input before including it in a HTML report, which could let a remote malicious user execute arbitrary HTML or script code.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Trend Micro Scanning Engine Report Generation HTML Injection |
| High | WildTangent, Inc.[15]<br><br>WebDriver 4.0 | A buffer overflow vulnerability exists due to boundary errors within various functions in the 'WTHoster' and 'WebDriver' modules, which could let a remote malicious user execute arbitrary code.<br><br>Upgrade available at:<br>http://www.wildtangent.com/default.asp?pageID=webdriver_download<br><br>Currently we are not aware of any exploits for this vulnerability. | WebDriver Remote Filename Buffer Overflow |

[14] Bugtraq, June 3, 2004.

[15] NGSSoftware Insight Security Research Advisory, May 27, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **High/**<br>Medium<br><br>(High if arbitrary code can be executed) | e107.org[16]<br><br>e107 website system 0.6 15a, 0.6 15 | Multiple vulnerabilities exist: a vulnerability exists due to missing or insufficient input validation of various parameters in multiple PHP scripts, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in 'secure_img_render.php' due to insufficient verification of user input passed to the 'p' parameter before being used in include files, which could let a remote malicious user execute arbitrary scripts; a vulnerability exists in 'content.php' and 'news.php' due to insufficient sanitization of user input passed to certain parameters before being used in SQL queries, which could let a malicious user execute arbitrary SQL code; and a vulnerability exists because it is possible to disclose the absolute path to scripts in error pages by accessing them directly, which could let a remote malicious user obtain sensitive information.<br><br>Upgrades available at:<br>http://e107.org/download.php?view.50<br><br>Proofs of Concept exploits have been published. | e107 Website System Multiple Vulnerabilities |
| **High/**<br>Medium<br><br>(High if arbitrary code can be executed) | Sambar Technologies[17]<br><br>Sambar Server 6.1 beta 2 | Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of the 'show' parameter in 'sysadmin/system/show.asp' and the 'title' parameter in 'sysadmin/system/showperf.asp', which could let a remote malicious user execute arbitrary HTML and script code; and a Directory Traversal vulnerability exists in 'sysadmin/system/showini.asp' due to insufficient input validation, which could let a remote malicious user obtain sensitive information.<br><br>No workaround or patch available at time of publishing.<br><br>A Proof of Concept exploit has been published. | Sambar Server Multiple Vulnerabilities |
| Medium | Francisco Burzi[18]<br>osCommerce<br>Paul Laudanski<br>Trustix[19]<br><br>PHP-Nuke 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5, RC1-RC3, 6.5 FINAL, 6.5 BETA 1, 6.6, 6.7, 6.9, 7.0 FINAL, 7.0-7.3; osCommerce Osc2Nuke 7x 1.0; Paul Laudanski BetaNC PHP-Nuke Bundle;<br>Trustix Secure Enterprise Linux 2.0, Secure Linux 2.1 | A vulnerability exists due to improper validation of the location and name of the file being accessed, which could let a remote malicious user obtain sensitive information.<br><br>**Trustix:**<br>http://http.trustix.org/pub/trustix/updates/<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | PHP-Nuke Direct Script Access |

[16] waraxe-2004-SA#031, May 29, 2004.
[17] Secunia Advisory, SA11748, June 2. 2004.
[18] Bugtraq, June 1, 2004.
[19] Trustix Secure Linux Security Advisory, TSLSA-2004-0032, June 2, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | Hewlett Packard Company[20, 21]<br>OpenView Select Access 5.0 Patch 4, 5.1 Patch 1, 5.2, 6.0 | A vulnerability exists because UTF-8 encoded Unicode characters are not properly decoded in a URL, which could let a remote malicious user obtain unauthorized access.<br>Patches available at: http://support.openview.hp.com/cpe/select_access/patch_sa.jsp<br>Vulnerability may be exploited via a web browser. | OpenView Select Access Unicode Remote Access |
| Medium | IBM[22]<br>Tivoli Access Manager for e-business 3.9, 4.1, 5.1, Tivoli Access Manager Identity Manager Solution 5.1, Tivoli Configuration Manager 4.2, Tivoli Configuration Manager for ATM 2.1, Tivoli SecureWay Policy Director 3.8, WebSphere Everyplace Server 2.1.3-2.15 | A vulnerability exists due to an error related to the usage of cookies to maintain session connection information when logging in via forms authentication, which could let a remote malicious user obtain unauthorized access.<br>Patches available at: http://www-1.ibm.com/support/<br>Currently we are not aware of any exploits for this vulnerability. | IBM Multiple Product Unspecified Credential Impersonation |
| Medium | Microsoft[23]<br>Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4 | A vulnerability exists because accounts with expired passwords, in certain circumstances, can log on to a Windows 2000 domain, which could let a remote malicious user bypass security restrictions. Successful exploitation requires that the FQDN (Fully Qualified Domain Name) is exactly 8 characters long.<br>Microsoft has issued a hotfix, available from Microsoft Product Support Services (PSS). PSS contact information is available at: http://support.microsoft.com/default.aspx?scid=fh;[LN];CNTACTMS<br>There is not exploit code required. | Windows 2000 Domain Expired Account Security Policy Violation |
| Medium | Microsoft[24]<br>Internet Explorer 6.0 SP1 | A security vulnerability exists which could let a remote malicious user obtain unauthorized access to local resources on a client computer.<br>No workaround or patch available at time of publishing.<br>Proofs of Concept exploits have been published. Exploits are also circulating in the wild. | Internet Explorer URL Local Resource Access |

[20] HP Security Bulletin, HPSBMA01045, May 26, 2004.
[21] VU#205766, http://www.kb.cert.org/vuls/id/205766.
[22] SecurityFocus, June 2, 2004.
[23] Bugtraq, May 31, 2004.
[24] Securiteam, June 7, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | Opera Software[25]<br><br>Opera Web Browser 7.23, 7.50 | A vulnerability exists due to an error in the displaying of favicons in the address bar, page bar, and page/window cycler, which could let a malicious user spoof address bar information.<br><br>Upgrades available at:<br>http://www.opera.com/download/<br><br>There is not exploit code required. | Opera Browser Favicon Address Bar Spoofing |
| Medium | Rit Research Labs[26]<br><br>TinyWeb 1.9.2 | A vulnerability exists due to an input validation error that causes content in 'cgi-bin/' to be treated as non-executable files, which could let a remote malicious user bypass standard web server rules and obtain sensitive information.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | TinyWeb Server Remote CGI Script Disclosure |
| Medium | Sun Microsystems, Inc.[27]<br><br>Java System Application Server 7.0 Standard Edition, 7.0 Platform Edition, 7.0 Enterprise Edition, 8.0 Platform Edition | A installation path disclosure vulnerability exists due to a failure to properly filter user requests, which could let a remote malicious user obtain sensitive information.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Sun Java System Application Server Remote Installation Path Disclosure |
| Medium/ Low<br><br>(Medium if sensitive information can be obtained) | Microsoft[28]<br><br>Visual Studio .Net Microsoft Outlook 2003, Office 2003 Small Business Edition, 2003 Professional Edition,<br>Microsoft Business Solutions CRM 1.x | A Directory Traversal vulnerability exists in Crystal Reports and Crystal Enterprise from Business Objects due to an input validation error when handling HTTP requests, which could let a malicious user obtain sensitive information and cause a Denial of Service.<br><br>Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/security/bulletin/ms04-017.mspx<br><br>Currently we are not aware of any exploits for this vulnerability. | Crystal Reports Web Viewer Directory Traversal<br><br>CVE Name: CAN-2004-0204 |
| Low | Codemasters Software Company Limited[29]<br><br>Colin McRae Rally 04 | A remote Denial of Service vulnerability exists when the server returns a value to the target client for the 'numplayers' variable that is too high.<br><br>No workaround or patch available at time of publishing.<br><br>Exploit script has been published. | Colin McRae Rally 2004 Multiplayer Remote Denial of Service |

[25] GreyMagic Security Advisory, GM#007-OP, June 3, 2004.
[26] Securiteam, June 2, 2004.
[27] Bugtraq, May 27, 2004.
[28] Microsoft Security Bulletin, MS04-017, June 8, 2004.
[29] Securiteam, June 6, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Low | Hewlett Packard Company[30]<br><br>Integrated Lights Out 1.6A, 1.10, 1.15A, 1.15, 1.20A, 1.26A, 1.27A, 1.40A, 1.41A, 1.42A, 1.50A, 1.50, 1.51A | A remote Denial of Service vulnerability exists when LAN management products use TCP port 0 to access the iLO service.<br><br>Upgrade available at:<br>http://h18004.www1.hp.com/support/files/lights-out/us/index.html<br><br>There is not exploit code required. | Integrated Lights Out<br>Remote<br>Denial of Service |
| Low | Masato Kataoka[31]<br><br>Orenosv HTTP/FTP Server 0.5.9 f, 0.5.9e, 0.5.9 c | A remote Denial of Service vulnerability exists due to a boundary error within the HTTP service when handling requests.<br><br>Upgrade available at:<br>http://home.comcast.net/~makataoka/orenosv060.zip<br><br>A Proof of Concept exploit has been published. | Orenosv HTTP/FTP Server<br>Remote<br>Denial of Service |
| Low | Microsoft[32]<br><br>Windows 2000 Datacenter Server, Advanced Server, Professional, 2000 Server, Windows 98/SE/ME, Windows Server 2003 Datacenter Edition, Enterprise Edition, Standard Edition, Web Edition, XP Home Edition, XP Professional | A remote Denial of Service vulnerability exists in the in the IDirectPlay4 Application Programming Interface (API) of Microsoft DirectPlay due to insufficient validation of packets.<br><br>Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/security/bulletin/ms04-016.mspx<br><br>Currently we are not aware of any exploits for this vulnerability. | Microsoft DirectX DirectPlay Input Validation Remote Denial of Service<br><br>CVE Name:<br>CAN-2004-0202 |
| Low | MiniShare[33]<br><br>Minimal HTTP Server 1.3.2 | A remote Denial of Service vulnerability exists due to a failure to handle improperly formed HTTP requests.<br><br>Upgrade available at:<br>http://osdn.dl.sourceforge.net/sourceforge/minishare/minishare-1.3.3.exe<br><br>There is no exploit code required; however, a Proof of Concept exploit has been published. | MiniShare Server<br>Remote<br>Denial of Service |
| **High** | **Microsoft[34]**<br><br>**Outlook 2003**<br><br>***Exploit has been published.***[35] | **A media file script execution vulnerability due to a design error would allow for the execution of scripts located in media files regardless of security settings. This issue might allow a malicious user to execute arbitrary files on the affected computer.**<br><br>**No workaround or patch available at time of publishing.**<br><br>***Exploit script has been published.*** | **Microsoft Outlook 2003 Media File Script Execution Vulnerability** |

[30] HP Security Bulletin, HPSBMA01046, May 26, 2004.
[31] SP Research Labs Advisory x13, May 25, 2004.
[32] Microsoft Security Bulletin, MS04-016, June 8, 2004.
[33] Bugtraq, May 26, 2004.
[34] Security Focus, May 17, 2004
[35] SecurityFocus, May 26, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High/Low<br>(High if arbitrary code can be executed) | Apache Software Foundation[36]<br>*Mandrake*[37]<br>*OpenPKG*[38]<br>*Tinysofa*[39]<br>*Trustix*[40]<br>Apache 1.3-2.0.49<br>*Vendor advisories issued and patches now available* | A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a Denial of Service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.<br>No workaround or patch available at time of publishing.<br>Currently we are not aware of any exploits for this vulnerability.<br>*Patch available at:*<br>http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&r2=1.106<br>*Mandrake:*<br>http://www.mandrakesecure.net/en/ftp.php<br>*OpenPKG:*<br>ftp://ftp.openpkg.org<br>*Tinysofa:*<br>http://www.tinysofa.org/support/errata/2004/008.html<br>*Trustix:*<br>http://http.trustix.org/pub/trustix/updates/ | Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability<br>CVE Name: CAN-2004-0488 |

[36] Security Focus, May 17, 2004

[37] Mandrakelinux Security Update Advisories, MDKSA-2004:054 & 055, June 1. 2004.

[38] OpenPKG Security Advisory, OpenPKG-SA-2004.026, May 27, 2004.

[39] Tinysofa Security Advisory, TSSA-2004-008, June 2, 2004.

[40] Trustix Security Advisory, TSLSA-2004-0031, June 2, 2004.

| Risk* | Vendor<br>&<br>Software Name | Windows Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High/Low<br>(High if arbitrary code can be executed) | Multiple Vendors[41]<br>Apple<br>*Gentoo*[42]<br>iCab Company<br>KDE<br>MacWarriors<br>*Mandrake*[43]<br>Microsoft<br>Mozilla<br>Omni Group<br>Opera Software<br>Apple Safari Beta 2, 1.0, 1.1;<br>iCab Company iCab 2.9.8, Pre 2.7-2.71;<br>KDE KDE 3.1.4, 3.1.5, kdelibs 2.0, 2.0.1, 2.1-2.1.2, 3.1-3.1.3, 3.2, 3.2.1, 3.2.2;<br>MacWarriors TrailBlazer 0.52;<br>Microsoft Internet Explorer 5.0-6.0;<br>Mozilla Firefox 0.8;<br>Omni Group OmniWeb 4.0.6-4.5;<br>Opera Software Opera Web Browser 7.23<br>*Vendors issue advisories* | A vulnerability exists that relates to the processing of URI requests via various protocol handlers including telnet, rlogin, ssh and mailto. Successful exploitation of this issue may allow a remote malicious user to create or modify arbitrary files, resulting in a Denial of Service condition in the browser. The attack would occur in the context of the user running the vulnerable browser.<br>No workaround or patch available at time of publishing.<br>There is not exploit code required; however, Proofs of Concept exploits have been published.<br>*Gentoo:*<br>*http://security.gentoo.org/glsa/glsa-200405-19.xml*<br>*Mandrake:*<br>http://www.mandrakesecure.net/en/advisories/ | Multiple Vendor URI Protocol Handler Arbitrary File Creation/ Modification |
| Medium | Multiple Vendors[44]<br>Microsoft Outlook Express 6.0;<br>Qualcomm Eudora 6.0 .22, 6.0, 6.0.1, 6.0.3, 6.1<br>*Upgrade now available*[45] | A vulnerability exists due to a failure to properly display the URL in the status bar if a specially crafted long URL containing multiple spaces, which could let a malicious user hide spoofed URLs.<br>No workaround or patch available at time of publishing.<br>Vulnerability is being actively exploited in the wild by an e-mail that is being spammed to end-users.<br>*Upgrade available at:*<br>http://www.eudora.com/products/eudora/download/windows.html | Eudora Embedded Hyperlink URI Obfuscation Weakness |

[41] Security Focus, May 13, 2004

[42] Gentoo Linux Security Advisory, GLSA 200405-19, May 25, 2004.

[43] Mandrakelinux Security Update Advisory, MDKSA-2004:047, May 18, 2004.

[44] SecurityFocus, May 7, 2004.

[45] SecurityFocus, May 21, 2004.

# *Unix Operating Systems*

| Risk* | Vendor & Software Name | Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts | Common Name |
|---|---|---|---|
| **High** | Bell Labs[46]<br>Unix Seventh Edition | A buffer overflow vulnerability exists in 'mkdir' which could let a malicious user execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>Exploit scripts have been published. | Mkdir Buffer Overflow |
| **High** | CPanel, Inc.[47]<br>cPanel 5.0, 5.3, 6.0, 6.2, 6.4, 6.4.1, 6.4.2 STABLE_48, 6.4.2, 7.0. 8.0, 9.0, 9.1 .0-R85, 9.1 | A vulnerability exists in cPanel when used with the Apache 'mod_phpsuexec' option, which could let a malicious user execute arbitrary code.<br>Customers are advised to contact the vendor for further details regarding obtaining and applying fixes. It is reported that only Apache configurations compiled before April 15, 2004 are vulnerable.<br>There is no exploit code required. | cPanel Apache 'mod_phpsuexec' Options |
| **High** | craftysyntax.com[48]<br>Crafty Syntax Live Help 2.7.3 | A Cross-Site Script vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code.<br>Upgrade available at:<br>http://prdownloads.sourceforge.net/cslive/CSLHv2.7.4.tar.gz?download<br>There is not exploit code required. | Crafty Syntax Live Help Multiple HTML Injection |
| **High** | e107.org[49]<br>e107 website system 0.6 10 -0.6 15a, 0.545, 0.554, 0.555 Beta, 0.603 | A Cross-Site Scripting vulnerability exists because 'usersettings.php' does not filter HTML code from user-supplied input before 'user.php' displays the information, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | e107 'usersettings.php' Cross-Site Scripting |
| **High** | EnderUNIX SDT[50]<br>Isoqlog 2.1.1, 2.2 beta | Multiple buffer overflow vulnerabilities exist due to boundary errors within several functions, which could let a remote malicious user execute arbitrary code.<br>Upgrades available at:<br>http://www.enderunix.org/isoqlog/isoqlog-2.2.tar.gz<br>Currently we are not aware of any exploits for this vulnerability. | Isoqlog Multiple Buffer Overflows |
| **High** | EnderUNIX SDT[51]<br>Spamguard 1.6 | Multiple buffer overflow vulnerabilities exist in various source files and functions, which could let a remote malicious user execute arbitrary code.<br>Upgrade available at:<br>http://www.enderunix.org/spamguard/spamguard-1.7-BETA.tar.gz<br>Currently we are not aware of any exploits for this vulnerability. | Spamguard Multiple Buffer Overflows |

[46] Bugtraq, June 2, 2004.
[47] Securiteam, May 24, 2004.
[48] Bugtraq, June 3, 2004.
[49] R.A.M Security Advisory, May 22, 2004.
[50] Bugtraq, May 28, 2004.
[51] Bugtraq, May 28, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| **High** | Gallery Project[52]<br>Debian[53]<br>Debian Linux 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;<br>Gallery Gallery 1.4 -pl1-pl2, 1.4-1.4.3 -pl1 | A vulnerability exists due to an authentication error, which could let a remote malicious user obtain administrative access.<br>Upgrades available at:<br>http://prdownloads.sourceforge.net/gallery/gallery-1.4.3-pl2.tar.gz?download<br>**Debian:**<br>http://security.debian.org/pool/updates/main/g/gallery/<br>There is not exploit code required. | Gallery 'init.php' Authentication Flaw |
| **High** | GNU[54]<br>Conectiva[55]<br>Mailman 1.0, 1.1, 2.0 beta 3-beta 5, 2.0-2.0.13, 2.1, 2.1b1, 2.1.1 | A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.<br>Upgrade available at:<br>http://ftp.gnu.org/gnu/mailman/mailman-2.1.3.tgz<br>**Conectiva:**<br>ftp://atualizacoes.conectiva.com.br/<br>There is no exploit code required. | GNU Mailman Cross-Site Scripting<br>CVE Name:<br>CAN-2003-0992 |
| **High** | Gregg Kenneth Jewell[56]<br>Mail Manage EX 3.1.8 | A vulnerability exists in the 'mmex.php' script due to insufficient validation of user-supplied input in the '$Settings' variable, which could let a remote malicious user execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Mail Manage EX Arbitrary File Inclusion |
| **High** | Joachim Wieland[57]<br>Debian<br>jftpgw 0.13-0.13.3 | A format string vulnerability exists due to the insecure usage of the 'syslog()' function, which could let a remote malicious user execute arbitrary code.<br>Upgrade available at:<br>http://www.mcknight.de/jftpgw/jftpgw-0.13.4.tar.gz<br>Debian:<br>http://security.debian.org/pool/updates/main/j/jftpgw/<br>Currently we are not aware of any exploits for this vulnerability. | jftpgw Format String<br>CVE Name:<br>CAN-2004-0448 |
| **High** | ldu.neocrome.net [58]<br>Land Down Under 700-01-03, 602, 601 | A Cross-Site Scripting vulnerability exists due to missing input validation of BBcode tags, which could let a remote malicious user execute arbitrary HTML and script code.<br>Upgrades available at:<br>http://ldu.neocrome.net/page.php?id=1357<br>A Proof of Concept exploit has been published. | Land Down Under BBCode Cross-Site Scripting |

[52] Gallery Security Release, June 1, 2004.
[53] Debian Security Advisory, DSA 512-1, June 2, 2004.
[54] SecurityFocus, May 25, 2004.
[55] Conectiva Linux Security Announcement, CLA-2004:842, May 25, 2004.
[56] Secunia Advisory, SA11774, June 3, 2004.
[57] Debian Security Advisory DSA 510-1, May 29, 2004.
[58] Securiteam, May 30, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| High | Michael Krax<br>Debian[59]<br><br>log2mail 0.2.2 .2, 0.2.5 .2, 0.2.5 .1, 0.2.5 .0, | A format string vulnerability exists in the 'printlog()' function when logging information, which could let a remote malicious user execute arbitrary code.<br><br>**Debian:**<br>http://security.debian.org/pool/updates/main/l/log2mail/<br><br>Currently we are not aware of any exploits for this vulnerability. | log2mail<br>Format String<br><br>CVA Name:<br>CAN-2004-0450 |
| High | MIT[60, 61]<br>Debian<br>Immunix<br>Mandrake[62]<br>OpenBSD<br>RedHat<br>Tinysofa[63]<br>Trustix[64]<br><br>Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2.1-1.2.7, 1.3 -alpha1, 5.0 -1.3.3, 5.0 -1.2beta1&2, 5.0 -1.1.1, 5.0 -1.1, 5.0 -1.0.x;<br>tinysofa enterprise server 1.0 -U1, 1.0 | Multiple buffer overflow vulnerabilities exist due to boundary errors within the 'krb5_aname_to_localname()' library function during conversion of Kerberos principal names into local account names, which could let a remote malicious user execute arbitrary code with root privileges.<br><br>Patch available at:<br>http://web.mit.edu/kerberos/advisories/2004-001-an_to_ln_patch.txt<br>**Mandrake:**<br>http://www.mandrakesoft.com/security/advisories<br>**Tinysofa:**<br>http://www.tinysofa.org/support/errata/2004/009.html<br>**Trustix:**<br>http://http.trustix.org/pub/trustix/updates/<br><br>Currently we are not aware of any exploits for this vulnerability. | Kerberos 5<br>'krb5_aname_to_localname'<br>Multiple<br>Buffer Overflows |
| High | Oracle Corporation[65]<br><br>Oracle Applications 11.0, E-Business Suite 11.0, E-Business Suite 11i 11.5.1-11.5.8 | Multiple vulnerabilities exist due to input validation errors, which could let a remote malicious user execute arbitrary code.<br><br>Patches available at:<br>http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=274375.1<br><br>There is not exploit code required. | Oracle<br>E-Business Suite<br>Multiple Input<br>Validation |
| High | Pawel Jaczewski[66]<br><br>JPortal Web Portal 2.2.1 | An input validation vulnerability exists in 'module/print.inc.php' due to insufficient filtering of user-supplied data, which could let a remote malicious user execute arbitrary SQL commands.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | JPortal<br>'Print.php'<br>SQL Injection |
| High | PHP Group<br>Slackware[67]<br><br>Linux 8.1, 9.0, 9.1 | A vulnerability exists because PHP is linked against a static library in an insecure path, which could let a malicious user execute arbitrary code.<br><br>Updates available at:<br>ftp://ftp.slackware.com/pub/slackware/<br><br>Currently we are not aware of any exploits for this vulnerability. | Slackware Linux<br>PHP Packages<br>Insecure Linking<br>Configuration |

[59] Debian Security Advisory, DSA 513-1, June 3, 2004.
[60] MIT krb5 Security Advisory 2004-001, June 3, 2004.
[61] TA04-147A, http://www.kb.cert.org/vuls/id/686862.
[62] Mandrakelinux Security Update Advisory, MDKSA-2004:056, June 3, 2004.
[63] Tinasofa Security Advisory, TSSA-2004-009, June 2, 2004.
[64] Trustix Security Advisory, TSLSA-2004-0032, June 2, 2004.
[65] Oracle Security Alert 67, June 3, 2004.
[66] Secunia Advisory, SA11737, May 31, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | PHP Group[68]<br>Apple<br>Caldera<br>Conectiva<br>Debian<br>Engarde<br>FreeBSD<br>Gentoo<br>HP<br>IBM<br>Mandrake<br>OpenPKG<br>RedHat<br>Slackware<br>Sun Microsystems<br>SuSE<br>Trustix<br><br>PHP 3.0, 3.0 .13-3.0 .18, 3.0.1-3.0.13, 3.0.16, 4.0, 4.0.1 pl1&pl2, 4.0.1-4.0.7, RC1-RC3, 4.1.0-4.1.2, 4.2 .0, 4.2 –dev, 4.2.1-4.2.3, 4.3-4.3.3, 4.3.6, 5.0 candidate 1 & 2 | A vulnerability exists in the PHP 'include()' function when an application uses a user-supplied URI parameter as an argument, which could let a remote malicious user execute arbitrary commands.<br><br>No workaround or patch available at time of publishing.<br><br>Exploit script has been published. | PHP 'include()' function Remote Command Execution |
| High | Real Networks[69]<br><br>RealPlayer G2, 6.0 Win32, 6.0 Unix, 7.0 Win32, 7.0 Unix, 7.0 Mac, 8.0 Win32, 8.0 Unix. 8.0 Mac, 10.0 BETA, 10.0 v6.0.12.690, RealPlayer for Windows 7.0 | A vulnerability exists in the default installations of RealPlayer, which could let a remote malicious user execute arbitrary code.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required. | RealNetworks RealPlayer Remote Code Execution |
| High | SGI[70]<br><br>IRIX 6.5.x | A vulnerability exists because the /usr/sbin/cpr binary can be forced to load a user provided library when restarting the checkpointed process, which could let a malicious user obtain root privileges.<br><br>Upgrade available at:<br>ftp://patches.sgi.com/support/free/security/advisories/<br><br>Currently we are not aware of any exploits for this vulnerability. | IRIX Checkpoint and Restart libcpr Library Error<br><br>CVE Name:<br>CAN-2004-0134 |

[67] Slackware Security Advisory, SSA:2004-154-02, June 3, 2004.
[68] Bugtraq, May 27, 2004.
[69] SecurityTracker Alert, 1010396, June 4, 2004.
[70] SGI Security Advisory, 20040507-01-P, May 26, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| High | SquirrelMail Development Team[71]<br>Open Webmail<br><br>SquirrelMail 1.4-1.4.3 RC1, 1.5 Development Version;<br>Open Webmail 2.30-2.32 | A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied e-mail header strings, which could let a remote malicious user execute arbitrary code.<br><br>Upgrades available at:<br>http://www.squirrelmail.org/download.php<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published. | SquirrelMail Cross-Site Scripting |
| High | SquirrelMail Development Team[72]<br>Gentoo[73]<br><br>SquirrelMail 1.0.4, 1.0.5, 1.2.0-1.2.11, 1.4-1.4.2 | A vulnerability exists due to input validation errors, which could let a remote malicious user execute arbitrary HTML and script code.<br><br>Upgrades available at:<br>http://sourceforge.net/project/showfiles.php?group_id=311&package_id=334&release_id=237332<br><br>There is no exploit code required. | SquirrelMail SQL Injection |

[71] RS-2004-1, May 30, 2004.
[72] Secunia Advisory, SA11685, May 21, 2004.
[73] Gentoo Linux Security Advisories, GLSA 200405-16 & 16:02, May 21 & 25, 2004.

| Risk* | Vendor & Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | Trend Micro[74]<br>InterScan VirusWall 3.0.1, 3.2.3, 3.3, 3.6, Build 1166, Build 1182, 3.7, Build 1190, 3.8 Build 1130, 3.32, 3.52, (HP-UX) 3.6, (Linux) 3.0.1, (Linux) 3.6, (Solaris) 3.6 Unix 3.0.1, 3.6 x, Windows NT 3.4, 3.5, 3.6, 3.51, 3.52, build 1466, 5.1, InterScan WebManager 1.2, 2.0, 2.1, OfficeScan Corporate Edition 3.0, 3.5, 3.11, 3.13, 3.54, 5.02, 5.58, OfficeScan Corporate Edition for Windows NT Server 3.0, 3.1.1, 3.5, 3.11, 3.13, OfficeScan For Microsoft SBS 4.5, Micro PC-cillin 2003, 2002, 2000, 6.0, ScanMail 1.0, ScanMail for Microsoft Exchange 3.8, 3.81, 6.1, Scanning Engine 7.1, Virus Buster Corporate Edition 3.52-3.54, Virusbuster 2001 8.0.1, 8.0.2, Viruswall 3.0.1 | A vulnerability exists due to insufficient sanitization of user-supplied input before including it in a HTML report, which could let a remote malicious user execute arbitrary HTML or script code.<br>No workaround or patch available at time of publishing.<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Trend Micro Scanning Engine Report Generation HTML Injection |
| High | Tripwire, Inc.[75]<br>Gentoo[76]<br>Tripwire 2.2.1, 2.3.0, 2.3.1 -2, 2.3.1, 2.4 .0, 2.4.2, 3.0 1, 3.0, 4.0, 4.0.1, 4.1, 4.2, Tripwire Open Source 2.3.0, 2.3.1 | A format string vulnerability exists in 'pipedmailmessage.cpp' when an e-mail report is generated, which could let a malicious user execute arbitrary code. *Note: It is reported that this issue only presents itself when the MAILMETHOD is sendmail.*<br>Patch available at:<br>http://www.securityfocus.com/bid/10454/solution/<br>**Gentoo:**<br>http://security.gentoo.org/glsa/glsa-200406-02.xml<br>Currently we are not aware of any exploits for this vulnerability. | Tripwire Email Reporting Format String |

[74] Bugtraq, June 3, 2004.
[75] SecurityFocus, June 5, 2004.
[76] Gentoo Linux Security Advisory, GLSA 200406-02, June 4, 2004.

| Risk* | Vendor & Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **High/** Medium<br>(High if arbitrary code can be executed) | e107.org[77]<br>e107 website system 0.6 15a, 0.6 15 | Multiple vulnerabilities exist: a vulnerability exists due to missing or insufficient input validation of various parameters in multiple PHP scripts, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in 'secure_img_render.php' due to insufficient verification of user input passed to the 'p' parameter before being used in include files, which could let a remote malicious user execute arbitrary scripts; a vulnerability exists in 'content.php' and 'news.php' due to insufficient sanitization of user input passed to certain parameters before being used in SQL queries, which could let a malicious user execute arbitrary SQL code; and a vulnerability exists because it is possible to disclose the absolute path to scripts in error pages by accessing them directly, which could let a remote malicious user obtain sensitive information.<br>Upgrades available at:<br>http://e107.org/download.php?view.50<br>Proofs of Concept exploits have been published. | e107 Website System Multiple Vulnerabilities |
| **High**/Low<br>(High if arbitrary code can be executed) | Firebird[78]<br>Firebird 1.0 | A buffer overflow vulnerability exists when handling database names due to insufficient boundary checks, which could let a remote malicious user cause a Denial of Service and ultimately execute arbitrary code.<br>Upgrade available at:<br>http://firebird.sourceforge.net/index.php?op=files&id=engine<br>A Proof of Concept exploit has been published. | Firebird Remote Database Name Buffer Overflow |
| **High**/Low<br>(High if arbitrary code can be executed) | l2tpd.org[79]<br>Debian<br>l2tpd 0.62-0.69 | A buffer overflow vulnerability exists in the 'write_packet()' function due to a failure of the application to properly validate user supplied string lengths, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>Currently we are not aware of any exploits for this vulnerability. | L2TPD Buffer Overflow |
| Medium | cPanel, Inc.[80]<br>cPanel 5.0, 5.3, 6.0, 6.2, 6.4, 6.4.1, 6.4.2 .STABLE_48, 6.4.2, 7.0, 8.0, 9.0, 9.1 .0-R85, 9.1 | A vulnerability exists due to an error within the '/scripts/killacct' script, which could let a remote authenticated malicious administrator delete customer account DNS information for customers that are not administered by that administrator.<br>Customers are advised to contact the vendor for further information regarding obtaining and installing RELEASE builds.<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | cPanel '/scripts/killacct' Script Customer Account DNS Information Deletion |

[77] waraxe-2004-SA#031, May 29, 2004.
[78] Securiteam, June 1, 2004.
[79] Bugtraq, June 4, 2004.
[80] SecurityTracker Alert, 1010398, June 4, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | Francisco Burzi[81]<br>osCommerce<br>Paul Laudanski<br>Trustix[82]<br>PHP-Nuke 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5, RC1-RC3, 6.5 FINAL, 6.5 BETA 1, 6.6, 6.7, 6.9, 7.0 FINAL, 7.0-7.3; osCommerce Osc2Nuke 7x 1.0; Paul Laudanski BetaNC PHP-Nuke Bundle; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.1 | A vulnerability exists due to improper validation of the location and name of the file being accessed, which could let a remote malicious user obtain sensitive information.<br>**Trustix:**<br>http://http.trustix.org/pub/trustix/updates/<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | PHP-Nuke Direct Script Access |
| Medium | FreeBSD[83]<br>FreeBSD 4.0-RELENG, 4.8-RELENG, 4.8-RELEASE-p7, 4.8-PRERELEASE, 4.8, 4.9-RELENG, 4.9-PRERELEASE, 4.9, 4.10-RELENG, 4.10-RELEASE, 4.10, 5.2-RELENG, 5.2-RELEASE, 5.2, 5.2.1-RELEASE | A vulnerability exists due to programming errors within the 'msync()' system call when performing MS_INVALIDATE operations, which could let a malicious user prevent modifications made to a file from being written to disk.<br>Patches available at:<br>ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync4.patch<br>ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync4.patch.asc<br>Currently we are not aware of any exploits for this vulnerability. | FreeBSD Msync(2) System Call Error<br>CVE Name:<br>CAN-2004-0435 |
| Medium | gatos[84]<br>Debian<br>gatos .5 | A vulnerability exists due to an error within 'xatitv' during initialization, which could let a malicious user obtain elevated privileges.<br>Upgrades available at:<br>http://security.debian.org/pool/updates/main/g/gatos/<br>There is not exploit code required. | Gatos 'xatitv' Elevated Privileges<br>CVE Name:<br>CAN-2004-0395 |

[81] Bugtraq, June 1, 2004.
[82] Trustix Secure Linux Security Advisory, TSLSA-2004-0032, June 2, 2004.
[83] FreeBSD Security Advisory, FreeBSD-SA-04:11, May 26,2 004.
[84] Debian Security Advisory, DSA 509-1, May 29, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | Gerd Knorr<br>Debian[85]<br>Mandrake[86]<br><br>xpcd 2.0 8; Debian Linux 3.0, alpha, arm, hppa, ia-32, ia-64, m68k, mips, mipsel, ppc, s/390, sparc,; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64 | A buffer overflow vulnerability exists in the 'pcd_open()' function in 'libpcd/file.c' in the xpcd-svga component due to insufficient bounds checking, which could let a malicious user obtain elevated privileges.<br><br>**Debian:**<br>http://security.debian.org/pool/updates/main/x/xpcd/<br>**Mandrake:**<br>http://www.mandrakesecure.net/en/ftp.php<br><br>There is no exploit code required. | XPCD-SVGA Buffer Overflow<br><br>CVE Name:<br>CAN-2004-0402 |
| Medium | GNU[87]<br>Conectiva [88]<br>Mandrake[89]<br><br>Mailman 1.0, 1.1, 2.0 beta 3-beta 5, 2.0-2.0.13, 2.1, 2.1b1, 2.1.1-2.1.4 | A vulnerability exists because a remote malicious user can send a specially crafted e-mail request to the mailman server to retrieve the mailman password of a target mailman subscriber.<br><br>Upgrade available at:<br>http://prdownloads.sourceforge.net/mailman/mailman-2.1.5.tgz?download<br>**Conectiva:**<br>ftp://atualizacoes.conectiva.com.br/9/RPMS/mailman-2.1.4-27744U90_2cl.i386.rpm<br>**Mandrake:**<br>http://www.mandrakesecure.net/en/ftp.php<br><br>Currently we are not aware of any exploits for this vulnerability. | GNU Mailman Password Retrieval<br><br>CVE Name:<br>CAN-2004-0412 |
| Medium | Hewlett Packard Company[90, 91]<br><br>OpenView Select Access 5.0 Patch 4, 5.1 Patch 1, 5.2, 6.0 | A vulnerability exists because UTF-8 encoded Unicode characters are not properly decoded in a URL, which could let a remote malicious user obtain unauthorized access.<br><br>Patches available at:<br>http://support.openview.hp.com/cpe/select_access/patch_sa.jsp<br><br>Vulnerability may be exploited via a web browser. | OpenView Select Access Unicode Remote Access |

[85] Debian Security Advisory, DSA 508-1, May 21, 2004.
[86] Mandrakelinux Security Update Advisory, MDKSA-2004:053, June 1, 2004.
[87] SecurityTracker Alert, 1010283, May 25, 2004.
[88] Conectiva Linux Security Announcement, CLA-2004:842, May 25, 2004.
[89] Mandrakelinux Security Update Advisory, MDKSA-2004:051, May 26, 2004.
[90] HP Security Bulletin, HPSBMA01045, May 26, 2004.
[91] VU#205766, http://www.kb.cert.org/vuls/id/205766.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | IBM[92]<br>Tivoli Access Manager for e-business 3.9, 4.1, 5.1, Tivoli Access Manager Identity Manager Solution 5.1, Tivoli Configuration Manager 4.2, Tivoli Configuration Manager for ATM 2.1, Tivoli SecureWay Policy Director 3.8, WebSphere Everyplace Server 2.1.3-2.15 | A vulnerability exists due to an error related to the usage of cookies to maintain session connection information when logging in via forms authentication, which could let a remote malicious user obtain unauthorized access.<br>Patches available at:<br>http://www-1.ibm.com/support/<br>Currently we are not aware of any exploits for this vulnerability. | IBM Multiple Product Unspecified Credential Impersonation |
| Medium | Pimentech[93]<br>PimenGest2 1.10 -1 | A vulnerability exists in 'rowLatex.inc.php' related to debug information, which could let a remote malicious user obtain sensitive information.<br>Upgrade available at:<br>ftp://ftp.pimentech.net/src/pimengest2.tgz<br>There is no exploit code required. | PimenGest2 'rowLatex.inc.php' Information Disclosure |
| Medium | Sun Microsystems, Inc.[94]<br>Java System Application Server 7.0 Standard Edition, 7.0 Platform Edition, 7.0 Enterprise Edition, 8.0 Platform Edition | An installation path disclosure vulnerability exists due to a failure to properly filter user requests, which could let a remote malicious user obtain sensitive information.<br>No workaround or patch available at time of publishing.<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Sun Java System Application Server Remote Path Disclosure |
| Medium | XFree86 Project[95]<br>OpenBSD<br>xdm CVS | A vulnerability exists in xdm because even though 'DisplayManager.requestPort' is set to 0, xdm will open a 'chooserFd' TCP socket on all interfaces, which could lead to a false sense of security.<br>Patch available at:<br>ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/008_xdm.patch<br>Currently we are not aware of any exploits for this vulnerability. | XFree86 XDM RequestPort False Sense of Security |

[92] SecurityFocus, June 2, 2004.
[93] SecurityFocus, May 24, 2004.
[94] Bugtraq, May 27, 2004.
[95] Secunia Advisory, SA11723, May 30, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| Low | Hewlett Packard Company[96]<br><br>Integrated Lights Out 1.6A, 1.10, 1.15A, 1.15, 1.20A, 1.26A, 1.27A, 1.40A, 1.41A, 1.42A, 1.50A, 1.50, 1.51A | A remote Denial of Service vulnerability exists when LAN management products use TCP port 0 to access the iLO service.<br><br>Upgrade available at:<br>http://h18004.www1.hp.com/support/files/lights-out/us/index.html<br><br>There is not exploit code required. | Integrated Lights Out<br>Remote<br>Denial of Service |
| Low | Sun Microsystems, Inc.[97]<br><br>Sun Fire B1600 | A remote Denial of Service vulnerability exists when an ARP datagram is received on the Network Management Port.<br><br>Patch available at:<br>http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=114783&rev=03<br><br>There is not exploit code required. | Fire B1600 Network Management Port<br>Remote<br>Denial of Service |
| Unavailable | Apple[98]<br><br>Mac OS X 10.3-10.3.3, Mac OS X Server 10.3-10.3.3 | Multiple vulnerabilities exist: a vulnerability exists in 'AppleFileServer' regarding the use of SSH and reporting errors; a vulnerability exists in the NFS implementation when tracing system calls; a vulnerability exists in 'LoginWindow' due to improper handling of directory service lookups and console log files; a vulnerability exists within the TCP/IP stack implementation when handling out-of-sequence TCP packets; a vulnerability exists within Terminal when handling URLs; and a vulnerability exists that involves the package installation. The impact was not specified for any of these vulnerabilities.<br><br>Upgrades available at:<br>http://www.apple.com/support/downloads/macosxcombined1034update.html<br><br>http://www.apple.com/support/downloads/macosxcombinedserver1034update.html<br><br>http://www.apple.com/support/downloads/macosxupdate_10_3_4.html<br><br>Currently we are not aware of any exploits for this vulnerability. | Mac OS X<br>Multiple<br>Security<br>Vulnerabilities |

[96] HP Security Bulletin, HPSBMA01046, May 26, 2004.
[97] Sun(sm) Alert Notification**,** 57430, June 2, 2004.
[98] Apple Security Advisory, APPLE-SA-2004-05-28, May 28, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | **Concurrent Versions System**[99, 100]<br>**Caldera**<br>**Conectiva**<br>**Debian**[101]<br>***Fedora***[102, 103]<br>***FreeBSD***[104]<br>***Gentoo***[105]<br>**Immunix**<br>***Mandrake***[106]<br>**OpenBSD**<br>***OpenPKG***[107]<br>***NetBSD***[108]<br>***RedHat***[109]<br>***SGI***[110]<br>***Slackware***[111]<br>***SuSE***[112]<br>***TurboLinux***[113]<br><br>**CVS 1.11.15 and prior versions (stable); 1.12.7 and prior versions (feature); Gentoo Linux 1.4; NetBSD Current, 1.6-1.6.2**<br><br>***Vendors issue advisories*** | **A buffer overflow vulnerability exists when handling user-supplied input for entry lines with 'modified' and 'unchanged' flags, which could let a remote malicious user execute arbitrary code.**<br><br>**Update available at: http://ccvs.cvshome.org/servlets/ProjectDownloadList**<br>**Debian:**<br>**http://www.debian.org/security/2004/dsa-505**<br><br>**Exploit scripts have been published.**<br><br>***Fedora:***<br>**http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/**<br>**http://download.fedoralegacy.org/redhat/**<br>***FreeBSD:***<br>**ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:10/cvs.patch**<br>***Gentoo:***<br>**http://security.gentoo.org/glsa/glsa-200405-12.xml**<br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/advisories/**<br>***NetBSD***<br>**ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2004-008.txt.asc**<br>***OpenPKG:***<br>**ftp://ftp.openpkg.org/release/**<br>***RedHat:***<br>**http://rhn.redhat.com/errata/RHSA-2004-190.html**<br>***Slackware:***<br>**ftp://ftp.slackware.com/pub/slackware/**<br>***SGI:***<br>**ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/**<br>***SuSE:***<br>**ftp://ftp.suse.com/pub/suse/i386/update**<br>***TurboLinux:***<br>**ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/8/updates/** | **CVS Buffer Overflow**<br><br>**CVE Name:**<br>**CAN-2004-0396** |

[99] ematters Advisory 07/2004, May 19, 2004
[100] VU#192038, http://www.kb.cert.org/vuls/id/192038
[101] Debian Security Advisory, DSA 505-1, May 19, 2004.
[102] Fedora Update Notifications, FEDORA-2004-126 & 131, May 19, 2004.
[103] Fedora Legacy Update Advisory, FLSA:1620, June 4, 2004.
[104] FreeBSD Security Advisory, FreeBSD-SA-04:10, May 19, 2004.
[105] Gentoo Linux Security Advisory, GLSA 200405-12, May 20, 2004.
[106] Mandrakelinux Security Update Advisory, MDKSA-2004:048, May 19, 2004.
[107] OpenPKG Security Advisory, OpenPKG-SA-2004.022, May 19, 2004.
[108] NetBSD Security Advisory 2004-008, June 3, 2004.
[109] RedHat Security Advisory, RHSA-2004:190-14, May 19, 2004.
[110] SGI Security Advisory, 20040508-01-U, May 28, 2004.
[111] Slackware Security Advisory, SSA:2004-140-01, May 20, 2004.
[112] SUSE Security Announcement, SuSE-SA:2004:013, May 19, 2004.
[113] Turbolinux Security Advisory TLSA-2004-15, May 28, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | KDE[114]<br>*Conectiva*[115]<br>*Fedora*[116]<br>*Gentoo*[117]<br>*RedHat*[118]<br>*SGI*[119]<br>*Slackware*[120]<br>*SuSE*[121]<br><br>All versions of KDE up to KDE 3.2.2 inclusive.<br><br>*Vendors issue advisories* | The telnet, rlogin, ssh and mailto URI handlers in KDE do not check for '-' at the beginning of the hostname passed, which makes it possible to pass an option to the programs started y the handlers. A remote user can create a URL that, when loaded, will create or overwrite files on the target user's system.<br><br>Patches available at:<br>http://www.kde.org/info/security/advisory-20040517-1.txt<br><br>Exploit script has been published.<br><br>*Conectiva:*<br>ftp://atualizacoes.conectiva.com.br/<br>*Fedora:*<br>http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/<br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-11.xml<br>*RedHat:*<br>http://rhn.redhat.com/errata/RHSA-2004-222.html<br>*SGI:*<br>http://www.sgi.com/support/security/<br>*Slackware:*<br>ftp://ftp.slackware.com/pub/slackware/<br>*SuSE:*<br>ftp://ftp.suse.com/pub/suse/i386/update/ | URI Handler Vulnerabilities<br><br>CVE Name:<br>CAN-2004-0411 |
| High | Multiple Vendors<br>*Gentoo*[122]<br>Xine[123]<br>Slackware[124]<br><br>MPlayer 1.0 pre3try2;<br>xine-lib 1-rc3a-rc3c, 1-rc2, 1-beta1- beta11<br><br>*Gentoo issues advisory* | Several buffer overflow vulnerabilities exist in 'realrtsp' code shared between MPlayer and xine-lib, which could let a remote malicious user execute arbitrary code.<br><br>Mplayer:<br>http://mplayer.dev.hu/homepage/design6/dload.html<br>Slackware:<br>ftp://ftp.slackware.com/pub/slackware/<br>Xine:<br>http://xinehq.de/index.php/releases<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-24.xml | MPlayer/ Xine-Lib Multiple RealRTSP Buffer Overflows |

[114] KDE Security Advisory, May 17, 2004

[115] Conectiva Linux Security Announcement, CLA-2004:843, May 26, 2004.

[116] Fedora Security Advisories, FEDORA-2004-121 & 122, May 17 & 19, 2004.

[117] Gentoo Linux Security Advisory, GLSA 200405-11, May 19, 2004.

[118] RedHat Security Advisory, RHSA-2004:222-11, May 17, 2004.

[119] SGI Security Advisories, 20040508-01-U & 20040509-01-U, May 28, 2004.

[120] Slackware Security Advisory, SSA:2004-238-01, May 18, 2004.

[121] SUSE Security Announcement, SuSE-SA:2003:014, May 26, 2004.

[122] Gentoo Linux Security Advisory, GLSA 200405-24, May 28, 2004.

[123] Xine Security Advisory, XSA-2004-3, April 30, 2004.

[124] Slackware Security Advisory, SSA:2004-124-03, May 3, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High | Multiple Vendors<br>Debian[125]<br>Fedora [126]<br>*Gentoo*[127]<br>Mandrake[128]<br>RedHat [129]<br>*SGI*[130]<br>*Slackware*[131]<br>*SuSE*[132]<br><br>Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4_rc1-3, 1.4; Midnight Commander 4.5.40- 4.5.55, 4.6; SGI ProPack 2.3, 2.4<br><br>*More vendors issue advisories* | Multiple vulnerabilities exist including several buffer overflows, a format string vulnerability, and a temporary file and directory creation vulnerability, which could let a malicious user obtain unauthorized access, cause a Denial of Service, or execute arbitrary code.<br><br>Debian:<br>http://security.debian.org/pool/updates/main/m/mc<br>Fedora:<br>http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1<br>Mandrake:<br>http://www.mandrakesecure.net/en/ftp.php<br>RedHat:<br>ftp://updates.redhat.com/9/en/os/i386/mc-4.6.0-14.9.i386.rpm<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-21.xml<br>*SGI:*<br>ftp://patches.sgi.com/support/free/security/advisories<br>*Slackware:*<br>ftp://ftp.slackware.com/pub/slackware/<br>*SuSE:*<br>ftp://ftp.suse.com/pub/suse/i386/update/9 | Midnight Commander Multiple Unspecified Vulnerabilities<br><br>CVE Names:<br>CAN-2004-0226,<br>CAN-2004-0231,<br>CAN-2004-0232 |
| High | Squirrel Mail Development Team [133]<br>*Gentoo*[134]<br><br>Squirrel Mail 1.0.4, 1.0.5, 1.2.0-1.2.11, 1.4- 1.4.2<br><br>*Gentoo issues advisories* | A Cross-Site Scripting vulnerability exists due to an input validation error in 'compose.php' when handling input passed to the 'mailbox' parameter, which could let a remote malicious user execute arbitrary HTML and script code.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, a Proof of Concept exploit has been published.<br><br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-16.xml | SquirrelMail Folder Name Cross-Site Scripting |

[125] Debian Security Advisory, DSA 497-1, April 29, 2004.
[126] Fedora Update Notification, FEDORA-2004-112, April 30, 2004.
[127] Gentoo Linux Security Advisory, GLSA 200405-21, May 26, 2004.
[128] Mandrakelinux Security Update Advisory, MDKSA-2004:039, April 30, 2004.
[129] Red Hat Security Advisory, RHSA-2004:173-01, April 30, 2004.
[130] SGI Security Advisory, 20040508-01-U, May 28, 2004.
[131] Slackware Security Advisory, SSA:2004-136-01, May 17, 2004.
[132] SUSE Security Announcement, SuSE-SA:2004:012, May 14, 2004.
[133] Bugtraq, April 29, 2004.
[134] Gentoo Linux Security Advisories, GLSA 200405-16 & 16:02, May 21 & 25, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **High/ Medium**<br>**(High if arbitrary code can be executed)** | **Multiple Vendors**<br>***Conectiva***[135]<br>**Clearswift**<br>***Debian***[136]<br>***F-Secure***[137]<br>***Fedora***[138]<br>***Gentoo***[139]<br>**Mr. S.K.**<br>**RARLAB**<br>**RedHat**[140]<br>**Slackware**[141]<br>**Stalker**<br>**WinZip**<br>**Mr. S.K. LHA 1.14, 1.15, 1.17; RARLAB WinRar 3.20; RedHat lha-1.14i-9.i386. rpm; WinZip 9.0; Stalker CGPMcAfee 3.2**<br>***More vendor issue advisories*** | **Multiple vulnerabilities exist: two buffer overflow vulnerabilities exist when creating a carefully crafted LHA archive, which could let a remote malicious user execute arbitrary code; and several Directory Traversal vulnerabilities exist, which could let a remote malicious user corrupt/overwrite files in the context of the user who is running the affected LHA utility.**<br>**RedHat:**<br>**ftp://updates.redhat.com/9/en/os/i386/lha-1.14i-9.1.i386.rpm**<br>**Slackware:**<br>**ftp://ftp.slackware.com/pub/slackware/**<br>**Proofs of Concept exploits have been published.**<br>***Conectiva:***<br>**ftp://atualizacoes.conectiva.com.br/**<br>***Debian:***<br>**http://security.debian.org/pool/updates/non-free/l/lha/**<br>***F-Secure:***<br>**http://www.f-secure.com/security/fsc-2004-1.shtml**<br>***Fedora:***<br>**http://www.redhat.com/archives/fedora-announce-list/2004-May/msg00005.html**<br>***Gentoo:***<br>**http://security.gentoo.org/glsa/glsa-200405-02.xml** | **Multiple LHA Buffer Overflow/ Directory Traversal Vulnerabilities**<br>**CVE Names: CAN-2004-0234, CAN-2004-0235** |
| **High/Low**<br>**(High if arbitrary code can be executed)** | **Apache Software Foundation**[142]<br>***Mandrake***[143]<br>***OpenPKG***[144]<br>***Tinysofa***[145]<br>***Trustix***[146]<br>**Apache 1.3-2.0.49**<br>***Vendor advisories issued and patches now available*** | **A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a Denial of Service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.**<br>**No workaround or patch available at time of publishing.**<br>**Currently we are not aware of any exploits for this vulnerability.**<br>***Patch available at:***<br>**http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&r2=1.106**<br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/ftp.php**<br>***OpenPKG:***<br>**ftp://ftp.openpkg.org**<br>***Tinysofa:***<br>**http://www.tinysofa.org/support/errata/2004/008.html**<br>***Trustix:***<br>**http://http.trustix.org/pub/trustix/updates/** | **Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability**<br>**CVE Name: CAN-2004-0488** |

[135] Conectiva Linux Security Announcement, CLA-2004:840, May 7, 2004.

[136] Debian Security Advisory DSA 515-1 , June 5, 2004.

[137] F-Secure Security Bulletin, FSC-2004-1, May 26, 2004.

[138] Fedora Update Notification, FEDORA-2004-119, May 11, 2004.

[139] Gentoo Linux Security Advisory, GLSA 200405-02, May 9, 2004.

[140] Red Hat Security Advisory, RHSA-2004:179-01, April 30, 2004.

[141] Slackware Security Advisory, SSA:2004-125-01, May 5, 2004.

[142] Security Focus, May 17, 2004

[143] Mandrakelinux Security Update Advisories, MDKSA-2004:054 & 055, June 1. 2004.

[144] OpenPKG Security Advisory, OpenPKG-SA-2004.026, May 27, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| High/Low<br>(High if arbitrary code can be executed) | Multiple Vendors [147]<br>Apple<br>*Gentoo*[148]<br>iCab Company<br>KDE<br>MacWarriors<br>*Mandrake*[149]<br>Microsoft<br>Mozilla<br>Omni Group<br>Opera Software<br><br>Apple Safari Beta 2, 1.0, 1.1;<br>iCab Company iCab 2.9.8, Pre 2.7-2.71;<br>KDE KDE 3.1.4, 3.1.5, kdelibs 2.0, 2.0.1, 2.1-2.1.2, 3.1-3.1.3, 3.2, 3.2.1, 3.2.2;<br>MacWarriors TrailBlazer 0.52;<br>Microsoft Internet Explorer 5.0-6.0;<br>Mozilla Firefox 0.8;<br>Omni Group OmniWeb 4.0.6-4.5;<br>Opera Software Opera Web Browser 7.23<br><br>*Vendors issue advisories* | A vulnerability exists that relates to the processing of URI requests via various protocol handlers including telnet, rlogin, ssh and mailto. Successful exploitation of this issue may allow a remote malicious user to create or modify arbitrary files, resulting in a Denial of Service condition in the browser. The attack would occur in the context of the user running the vulnerable browser.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required; however, Proofs of Concept exploits have been published.<br><br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-19.xml<br>*Mandrake:*<br>http://www.mandrakesecure.net/en/advisories/ | Multiple Vendor URI Protocol Handler Arbitrary File Creation/ Modification |

[145] Tinysofa Security Advisory, TSSA-2004-008, June 2, 2004.
[146] Trustix Security Advisory, TSLSA-2004-0031, June 2, 2004.
[147] Security Focus, May 13, 2004
[148] Gentoo Linux Security Advisory, GLSA 200405-19, May 25, 2004.
[149] Mandrakelinux Security Update Advisory, MDKSA-2004:047, May 18, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **High/Low**<br>**(High if arbitrary code can be executed)** | **Royal Institute of Technology**<br>**FreeBSD**[150]<br>***Debian***[151]<br>***Gentoo***[152]<br>**KTH Heimdal 0.5-0.5.3, 0.6 .0, 0.6.1**<br>***More vendor advisories issued*** | **A vulnerability exists due to a pre-authentication flaw in the k5admind(8) Kerberos Key Distribution Center (KDC) interface in the processing of Kerberos 4 compatibility administration requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**<br>**Update available at:**<br>**ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.6.2.tar.gz**<br>**FreeBSD:**<br>**ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:09/kadmind.patch**<br>**Currently we are not aware of any exploits for this vulnerability.**<br>***Debian:***<br>**http://security.debian.org/pool/updates/main/h/heimdal/**<br>***Gentoo:***<br>**http://security.gentoo.org/glsa/glsa-200405-23.xml** | **Heimdal K5AdminD Remote Heap Buffer Overflow**<br>**CVE Name: CAN-2004-0434** |
| **Medium** | **Kolab**<br>**OpenPKG**[153]<br>**Mandrake**[154]<br>**Kolab Groupware Server 1.0, 1.0.1, 1.0.3, 1.0.5, 1.0.6, 1.0.7, 1.0.8**<br>**OpenPKG OpenPKG 2.0**<br>***Mandrake issues advisory*** | **A vulnerability exists because passwords are stored in plaintext format, which could let a malicious user obtain sensitive information.**<br>**Upgrades available at:**<br>**http://www.erfrakon.de/projects/kolab/download/**<br>**OpenPKG:**<br>**ftp://ftp.openpkg.org/release/2.0/UPD/kolab-20040217-2.0.2.src.rpm**<br>**There is not exploit code required.**<br>***Mandrake:***<br>**http://www.mandrakesoft.com/security/advisories** | **Groupware Server OpenLDAP Plaintext Password Storage** |

[150] FreeBSD Security Advisory, FreeBSD-SA-04:09.kadmind, May 5. 2004.
[151] Debian Security Advisory, DSA 504-1, May 18, 2004.
[152] Gentoo Linux Security Advisory, GLSA 200405-23, May 27, 2004.
[153] OpenPKG Security Advisory, OpenPKG-SA-2004.019, May 5, 2004.
[154] Mandrakelinux Security Update Advisory, MDKSA-2004:052, May 26, 2004.

| Risk* | Vendor & Software Name | Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | Multiple Vendors<br>Debian[155]<br>Mandrake[156]<br>*OpenPKG*[157]<br>*RedHat*[158]<br>*SGI*[159]<br>Slackware[160]<br>Trustix[161]<br><br>Debian Linux 3.0, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;<br>rsync 2.3.1, 2.3.2 - 1.3, 2.3.2 -1.2, sparc, PPC, m68k, intel, ARM, alpha, 2.3.2, 2.4.0, 2.4.1, 2.4.3- 2.4.6, 2.4.8, 2.5.0- 2.5.7, 2.6<br><br>*More vendors issue advisories* | A vulnerability exists due to insufficient sanitization of user-supplied path values, which could let a remote malicious user modify system information or obtain unauthorized access.<br><br>Debian:<br>http://security.debian.org/pool/updates/main/r/rsync<br>Mandrake:<br>http://www.mandrakesecure.net/en/ftp.php<br>Rsync:<br>http://rsync.samba.org/ftp/rsync/rsync-2.6.1.tar.gz<br>Slackware:<br>ftp://ftp.slackware.com/pub/slackware/<br>Trustix:<br>http://www.trustix.org/errata/misc/2004/TSL-2004-0024-rsync.asc.txt<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*OpenPKG:*<br>ftp://ftp.openpkg.org/release/<br>*RedHat:*<br>http://rhn.redhat.com/errata/RHSA-2004-192.html<br>*SGI:*<br>ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/ | RSync Path Validation<br><br>CVE Name: CAN-2004-0426 |
| Medium | Multiple Vendors<br>Fedora[162]<br>*Mandrake*[163]<br>*SuSE*[164]<br><br>Linux kernel 2.5.0-2.5.69, 2.6, 2.6 -test1- test11, 2.6.1, rc1&rc2, 2.6.2-2.6.5<br><br>*Mandrake issues advisory* | A vulnerability exists in the 'cpufreq_userspace' proc handler, which could let a malicious user obtain sensitive information.<br><br>Update available at:<br>http://www.kernel.org/pub/linux/kernel/<br>Fedora:<br>http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/<br>SuSE:<br>ftp://ftp.suse.com/pub/suse/x86_64/update/<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*Mandrake:*<br>http://www.mandrakesoft.com/security/advisories | Linux Kernel CPUFreq Proc Handler Information Disclosure<br><br>CVE Name: CAN-2004-0228 |

[155] Debian Security Advisory, DSA 499-1, May 2, 2004.
[156] Mandrakelinux Security Update Advisory, MDKSA-2004:042, May 11, 2004.
[157] OpenPKG Security Advisory , OpenPKG-SA-2004.025, May 21, 2004.
[158] RedHat Security Advisory, RHSA-2004:192-06, May 19, 2004.
[159] SGI Security Advisories, 20040508-01-U & 20040509-01, May 28, 2004.
[160] Slackware Security Advisory, SSA:2004-124-01, May 3, 2004.
[161] Trustix Secure Linux Security Advisory, 2004-0024, April 30, 2004.
[162] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[163] Mandrakelinux Security Update Advisory, MDKSA-2004:050, May 21, 2004.
[164] SUSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Medium | Multiple Vendors<br>Engarde[165]<br>Fedora[166]<br>Mandrake[167]<br>*SGI*[168]<br>Slackware[169]<br>SuSE[170]<br>*TurboLinux*[171]<br><br>Linux kernel 2.4, 2.4 .0-test1- test12, 2.4.1- 2.4.26, 2.6, 2.6 -test1-test12, 2.6.1, rc1&rc2, 2.6.2- 2.6.5<br><br>*More vendors issue advisories* | A vulnerability exists because memory is allocated for child processes but never freed, which could let a malicious user obtain sensitive information.<br><br>Engarde:<br>http://infocenter.guardiandigital.com/advisories/<br>Fedora:<br>http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/<br>Mandrake:<br>http://www.mandrakesecure.net/en/advisories/<br>Slackware:<br>ftp://ftp.slackware.com/pub/slackware/<br>SuSE:<br>ftp://ftp.suse.com/pub/suse/<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*SGI:*<br>ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/<br>*TurboLinux:*<br>ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux | Linux kernel do_fork() Memory Leakage<br><br>CVE Name:<br>CAN-2004-0427 |
| Medium | Multiple Vendors<br>*SGI*[172]<br>Slackware[173]<br>SuSE[174]<br>*TurboLinux*[175]<br><br>Linux kernel 2.4.0-test1- test12, 2.4-2.4.25<br><br>*More vendors issue advisories* | A buffer overflow vulnerability exists in the 'panic()' function call, which could let a malicious user obtain sensitive information.<br><br>Slackware:<br>ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/<br>SuSE:<br>ftp://ftp.suse.com/pub/suse/i386/update/<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*SGI:*<br>ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/<br>*TurboLinux:*<br>ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux | Linux Kernel Panic Function Call Buffer Overflow<br><br>CVE Name:<br>CAN-2004-0394 |

[165] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004.
[166] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[167] Mandrakelinux Security Update Advisory, MDKSA-2004:037, April 27, 2004.
[168] SGI Security Advisories, 20040508-01-U & 20040509-01, May 28, 2004.
[169] Slackware Security Advisory, SSA:2004-119-01, April 29, 2004.
[170] SUSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.
[171] TurboLinux Security Advisory, TLSA-2004-05-21, May 21, 2004.
[172] SGI Security Advisories, 20040508-01-U & 20040509-01, May 28, 2004.
[173] Slackware Security Advisory, SSA:2004-119-01, April 29, 2004.
[174] SUSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.
[175] TurboLinux Security Advisory, TLSA-2004-05-21, May 21, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| Medium | MySQL AB<br>Conectiva<br>Debian[176]<br>Engarde<br>FreeBSD<br>*Gentoo*[177]<br>HP<br>IBM<br>Immunix<br>Mandrake[178]<br>OpenBSD<br>OpenPKG [179]<br>RedHat<br>Trustix<br>Sun<br>SuSE<br><br>MySQL AB<br>MySQL 3.20.32 a, 3.22.26- 3.22.30, 3.22.32, 3.23.2- 3.23.5, 3.23.8- 3.23.10, 3.23.22- 3.23.34, 3.23.36- 3.23.56, 3.23.58, 4.0 .0- 4.0.15, 4.0.18, 4.1.0-0, 4.1 .0-alpha<br><br>*Gentoo issues advisory* | A vulnerability exists in the MySQL 'mysqld_multi' script due to insecure temporary file handling, which could let a malicious user obtain elevated privileges.<br><br>Debian:<br>http://security.debian.org/pool/updates/main/m/mysql/<br>Mandrake:<br>http://www.mandrakesecure.net/en/ftp.php<br>OpenPKG:<br>ftp://ftp.openpkg.org/release/2.0/UPD/mysql-4.0.18-2.0.1.src.rpm<br><br>There is not exploit code required.<br><br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-20.xml | MySQL 'mysqld_multi' Insecure Temporary File Handling<br><br>CVE Name:<br>CAN-2004-0388 |

[176] Debian Security Advisory, DSA 483-1, April 14, 2004.
[177] Gentoo Linux Security Advisory, GLSA 200405-20, May 25, 2004.
[178] Mandrakelinux Security Update Advisory, MDKSA-2004:034, April 20, 2004.
[179] OpenPKG Security Advisory, OpenPKG-SA-2004.014, April 14, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| **Medium** | **RSync**<br>**Debian**[180]<br>**Mandrake**[181]<br>***OpenPKG***[182]<br>***RedHat***[183]<br>***SGI***[184]<br>**Slackware185**<br>**Trustix186**<br><br>**RSync 2.3.1, 2.3.2 -1.3, 2.3.2 -1.2, sparc, PPC, m68k, intel, ARM, alpha, 2.3.2, 2.4.0, 2.4.1, 2.4.3- 2.4.6, 2.4.8, 2.5.0- 2.5.7, 2.6; Debian Linux 3.0, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; MandrakeSoft Corporate Server 2.1 x86_64, 2.1, Linux 9.1, ppc, 9.2, amd64, 10.0, Multi Network Firewall 8.2; RedHat Desktop 3.0, Enterprise Linux WS 3, WS 2.1, ES 3, ES 2.1, AS 3, AS 2.1, Linux Advanced Work Station 2.1**<br><br>***More vendors issue advisories*** | **A vulnerability exists due to insufficient sanitization of user-supplied path values, which could let a remote malicious user modify system information or obtain unauthorized access.**<br><br>**Debian:**<br>**http://security.debian.org/pool/updates/main/r/rsync**<br>**Mandrake:**<br>**http://www.mandrakesecure.net/en/ftp.php**<br>**Rsync:**<br>**http://rsync.samba.org/ftp/rsync/rsync-2.6.1.tar.gz**<br>**Slackware:**<br>**ftp://ftp.slackware.com/pub/slackware/**<br>**Trustix:**<br>**http://www.trustix.org/errata/misc/2004/TSL-2004-0024-rsync.asc.txt**<br><br>**Currently we are not aware of any exploits for this vulnerability.**<br><br>***OpenPKG:***<br>**ftp://ftp.openpkg.org/release/**<br>***RedHat:***<br>**http://rhn.redhat.com/errata/RHSA-2004-192.html**<br>***SGI:***<br>**ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/** | **RSync<br>Path Validation**<br><br>**CVE Name:<br>CAN-2004-0426** |

[180] Debian Security Advisory, DSA 499-1, May 2, 2004.
[181] Mandrakelinux Security Update Advisory, MDKSA-2004:042, May 11, 2004.
[182] OpenPKG Security Advisory, OpenPKG-SA-2004.025, May 21, 2004.
[183] RedHat Security Advisory, RHSA-2004:192-06, May 19, 2004.
[184] SGI Security Advisories, 20040508-01-U & 20040509-01-U, May 28, 2004.
[185] Slackware Security Advisory, SSA:2004-124-01, May 3, 2004.
[186] Trustix Secure Linux Security Advisory, 2004-0024, April 30, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common<br>Name |
|---|---|---|---|
| Low | Multiple Vendors<br>Debian[187]<br>*Fedora[188]*<br>*Gentoo[189]*<br>Mandrake [190]<br>OpenPKG [191]<br>RedHat [192]<br>*SGI[193]*<br>Slackware[194]<br>Trustix[195]<br><br>libpng 1.0, 1.0.5-1.0.14, libpng3 1.2 .0- 1.2.5; OpenPKG 1.3, 2.0; RedHat libpng-1.2.2-16.i386 .rpm, libpng-1.2.2-20.i386. rpm, libpng-devel-1.2.2-20.i386. rpm, ibpng10-1.0.13-11.i386. rpm, libpng10-1.0.13-8.i386. rpm, libpng10-devel-1.0.13-11.i386. rpm, libpng10-devel-1.0.13-8.i386. rpm; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1<br><br>*More vendors issue advisories* | A remote Denial of Service vulnerability exists when handling certain types of malformed PNG images.<br><br>Debian:<br>http://security.debian.org/pool/updates/main/libp/libpng/<br>Mandrake:<br>http://www.mandrakesecure.net/en/ftp.php<br>OpenPKG:<br>ftp://ftp.openpkg.org/release/<br>RedHat:<br>ftp://updates.redhat.com/9/en/os/i386/<br>Slackware:<br>ftp://ftp.slackware.com/pub/slackware/<br>Trustix:<br>http://www.trustix.org/errata/misc/2004/TSL-2004-0025-multi.asc.txt<br><br>Currently we are not aware of any exploits for this vulnerability.<br><br>*Fedora:*<br>http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1<br>*Gentoo:*<br>http://security.gentoo.org/glsa/glsa-200405-06.xml<br>*SGI:*<br>ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/ | LibPNG PNG Image Remote Denial of Service<br><br>CVE Name:<br>CAN-2004-0421 |

[187] Debian Security Advisory, DSA 498-1, April 30, 2004.
[188] Fedora Update Notifications, FEDORA-2004-105 & 106, May 14, 2004.
[189] Gentoo Linux Security Advisory, GLSA 200405-06, May 14, 2004.
[190] Mandrakelinux Security Update Advisory, MDKSA-2004:040, April 30, 2004.
[191] OpenPKG Security Advisory, OpenPKG-SA-2004.017, April 30, 2004.
[192] Red Hat Security Advisory, RHSA-2004:181-01, April 30, 2004.
[193] SGI Security Advisories, 20040508-01-U & 20040509-01, May 28, 2004.
[194] Slackware Security Advisory, SSA:2004-124-04, May 3, 2004.
[195] Trustix Secure Linux Security Advisory, TSLSA-2004-0025, April 30, 2004.

| Risk* | Vendor<br>&<br>Software Name | Unix Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **Low** | **Sun Microsystems, Inc.**[196]<br>***HP***[197]<br><br>**JRE & SDL (Linux Production Release) 1.4.2 _03, 1.4.2, JRE & SDK (Solaris Production Release) 1.4.2 _03, 1.4.2, JRE & SDK (Windows Production Release) 1.4.2 _03, 1.4.2**<br><br>***HP issues advisory*** | **A remote Denial of Service vulnerability exists in the 'decodeArrayLoop()' function in ISO2022_JP$Decoder.**<br><br>**Upgrades available at:**<br>**http://java.sun.com/j2se/1.4.2/download.html**<br><br>**Currently we are not aware of any exploits for this vulnerability.**<br><br>***HP:***<br>**http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin** | **Sun Java Runtime Environment Remote Denial of Service** |
| **Low** | **SuSE**[198]<br>**Mandrake**[199]<br><br>**Linux 8.1, 9.0, Linux Enterprise Server 8**<br><br>***Mandrake issues advisory*** | **A Denial of Service vulnerability exists due to improper file permissions on the '/proc/scsi/qla2300/Hba ApiNode' file.**<br><br>**Update available at:**<br>**ftp://ftp.suse.com/pub/suse**<br><br>**Currently we are not aware of any exploits for this vulnerability.**<br><br>***Mandrake:***<br>**http://www.mandrakesoft.com/security/advisories** | **Linux Kernel Denial of Service** |

## *Multiple/Other Operating Systems*

| Risk* | Vendor<br>&<br>Software Name | Multiple/Other Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **High** | 3Com[200]<br><br>OfficeConnect Remote 812 ADSL, Router 1.1.9 .4 | A vulnerability exists through the web configuration interface because a series of authentication attempts can be made that contain an arbitrary username and password combination, which could let a remote malicious user bypass the authentication process to obtain administrative access.<br><br>Disable the HTTP interface on the affected device. You can disable this interface to deny a malicious user the necessary vector required to exploit this issue. A tutorial on disabling the HTTP interface can be found at the following link:<br>http://www.3com.com/products/en_US/detail.jsp?tab=support&pathtype=support&sku=3CP4144<br><br>There is not exploit code required. | OfficeConnect Remote 812 ADSL Router Web Interface Authentication Bypass<br><br>CVE Name: CAN-2004-0477 |

[196] Sun(sm) Alert Notification, 57555, May 6, 2004.
[197] HP Security Bulletin, HPSBUX01044, May 26, 2004.
[198] SuSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.
[199] Mandrakelinux Security Update Advisory, MDKSA-2004:050, May 21, 2004.
[200] iDEFENSE Security Advisory, May 27, 2004.

| Risk* | Vendor<br>&<br>Software Name | Multiple/Other Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| **High** | Linksys[201]<br><br>Linksys WRT54G v1.0 1.42.3 (Firmware), v2.0 2.0 0.8 (Firmware), Sveasoft Samadhi2 2.0.8 .6sv | A vulnerability exists because the administrative web interface is accessible on the WAN interface, even though the remote administration functionality has been disabled, which could let a remote malicious user access the administration web page.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required. | Linksys WRT54G Router Remote Administration Access |
| **High** | RARLAB[202]<br><br>UnRar 2.60, 2.70, 2.71, 2.80, 2.90 | A vulnerability exists due to a failure to properly implement a formatted string function, which could let a remote malicious user execute arbitrary code.<br><br>Upgrades available at:<br>http://www.rarlab.com/rar_add.htm<br><br>An exploit RAR archive has been made public ally available. | UnRAR Format String |
| **High** | NetGear[203]<br><br>WG602 Access Point Firmware 1.04.0, 1.7.14 | A vulnerability exists because the device contains an undocumented default administrative account, which could let a remote malicious user obtain administrative access.<br><br>No workaround or patch available at time of publishing.<br><br>There is not exploit code required. | Netgear WG602 Wireless Access Point Default Backdoor Account |
| **High/** Medium<br><br>(High if arbitrary code can be executed) | NetGear[204]<br><br>RP114 3.26 | A vulnerability exists in the keyword blocking mechanism, which could let a remote malicious user bypass content filter functionality and possibly execute arbitrary code. This vulnerability may result in a false sense of security for a network administrator.<br><br>No workaround or patch available at time of publishing.<br><br>There is no exploit code required; however, a Proof of Concept exploit has been published. | Netgear RP114 Content Filter Bypass |
| **High**/Low<br><br>(High if arbitrary code can be executed) | Qualcomm[205]<br><br>Eudora Internet Mail Server for Mac OS 7 | A buffer overflow vulnerability exists due to insufficient boundary checks on data that is received on port 105, which could let a remote malicious user execute arbitrary code or cause a Denial of Service.<br><br>No workaround or patch available at time of publishing.<br><br>Currently we are not aware of any exploits for this vulnerability. | Eudora Internet Mail Server For Mac OS 7 Remote Buffer Overflow |
| Medium | PHPoto [206]<br><br>PHPoto 0.1.2, 0.2.5, 0.3.6, 0.4 .0-pre-1-pre-5 | A vulnerability exists in the 'Picture_view' script, which could let a remote malicious user obtain unauthorized access to view any pictures hosted on a site, regardless of the user's privileges.<br><br>Upgrades available at:<br>http://prdownloads.sourceforge.net/phpoto/PHPoto-0.4.0-pre-6.zip?download<br><br>There is not exploit code required. | PHPoto 'Picture_view' Script Unauthorized Access |

[201] Securiteam, June 2, 2004.
[202] SecurityFocus, May 31, 2004.
[203] Secunia Advisory, SA11773, June 7, 2004.
[204] Securiteam, May 25, 2004.
[205] SecurityFocus, May 31, 2004.
[206] SecurityFocus, May 29, 2004.

| Risk* | Vendor & Software Name | Multiple/Other Operating Systems<br>Vulnerability - Impact<br>Patches - Workarounds<br>Attacks Scripts | Common Name |
|---|---|---|---|
| Low | 3Com[207]<br>OfficeConnect Remote 812 ADSL Router, Router 1.1.9.4 | A buffer overflow vulnerability exists through the telnet port, which could let a remote malicious user cause a Denial of Service.<br>No workaround or patch available at time of publishing.<br>Currently we are not aware of any exploits for this vulnerability. | OfficeConnect Remote 812 ADSL Router Telnet Remote Buffer Overflow<br>CVE Name: CAN-2004-0476 |
| Low | Canon[208]<br>imageRUNNER 210, 210S | A remote Denial of Service vulnerability exists when a malicious user carries out multiple port scans against port 80.<br>No workaround or patch available at time of publishing.<br>There is not exploit code required. | ImageRUNNER Port Scan Remote Denial of Service |
| Low | VocalTec[209]<br>VGW120 Telephony Gateway, VGW480 Telephony Gateway | A remote Denial of Service vulnerability exists due to a flaw in the processing of H.323/H.225 protocol messages.<br>No workaround or patch available at time of publishing.<br>Exploit script has been published. | VGW120/ VGW480 Telephony Gateway Remote H.225 Denial of Service |
| Low | Linksys[210]<br>Linksys BEFSR41 v1/v2 (firmware 1.45.7, 1.44.2z & possibly prior) BEFSR41 v3, BEFSRU31, BEFSR11, BEFSX41, BEFSR81 v2/v3, BEFW11S4 v3, BEFW11S4 v4 | Denial of Service vulnerabilities exist due to insufficient sanitization of the 'sysPasswd', 'sysPasswdConfirm', and 'DomainName' parameters in the 'Gozila.cgi' script.<br>Updates available at: http://www.linksys.com/download/firmware.asp?fwid=3<br>There is not exploit code required; however, a Proof of Concept exploit has been published. | Multiple Linksys Routers 'Gozila.CGI' Denials of Service |

*"Risk" is defined by CyberNotes in the following manner:

**High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

**Medium** – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

**Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against

[207] iDEFENSE Security Advisory, May 26, 2004.
[208] SecurityTracker Alert, 1010297, May 26, 2004.
[209] SecurityTracker Alert, 1010268, May 24, 2004.
[210] Bugtraq, June 3, 2004.

mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

## Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 24 and June 8, 2004, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period 23 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| **June 8, 2004** | **analysis.tgz** | **Complete analysis of the 180 Solutions Trojan along with exploitation tools that demonstrate at least two new unpublished vulnerabilities in Microsoft Internet Explorer 6 that allow for arbitrary code execution.** |
| June 8, 2004 | tcpick-0.1.23.tar.gz | A textmode sniffer that can track TCP streams and saves the data captured in files or displays them in the terminal |
| June 7, 2004 | x1bpackV1.tar.gz | A series of scripts written by the author as an exercise into socket programming with Perl. Included are a port scanner with banner grabbing capabilities, a DNS service enumeration script with zone transfer, some brute forcing utilities, a CGI web scanner, and a couple of other utilities. |
| June 7, 2004 | subexp.c | Subversion 1.0.2 remote exploit that makes use of a stack overflow in the svn_time_from_cstring() function. |
| **June 5, 2004** | **foolpw.c** | **Script that exploits the FoolProof Security Program Administrative Password Recovery vulnerability.** |
| **June 4, 2004** | **colin_mcrae_rally_04_dos.zip** | **Exploit for the Colin McRae Rally 2004 Multiplayer Remote Denial of Service vulnerability.** |
| **June 3, 2004** | **pdp11mkdir.c** | **Script that exploits the Mkdir Buffer Overflow vulnerability.** |
| **June 3, 2004** | **unix-v7-mkdir.c** | **Script that exploits the Mkdir Buffer Overflow vulnerability.** |
| June 3, 2004 | scanlogd-2.2.4.tar.gz | A TCP port scan detection tool originally designed to illustrate various attacks an IDS developer has to deal with. |
| June 2, 2004 | kenny.c | An IRC bot that executes shell commands and reports back any further information. Single host allowance for command execution is possible. |
| **June 2, 2004** | **mollensoftLightweight.txt** | **A Proof of Concept exploit for the Lightweight FTP Server Remote Buffer Overflow vulnerability.** |
| May 30, 2004 | rrs-1.70.tar.gz | A reverse (connecting) remote shell that listens for incoming connections and connects out to a listener (rrs in listen mode). The listener will accept the connection and receive a shell from the remote host. |

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| May 28, 2004 | csr-exploitation.pdf | A tutorial that defines several of the common types of vulnerabilities together with their counterpart command line exploit sequences. The descriptions of these types of vulnerabilities range from stack to heap, function pointer and format string weaknesses. |
| **May 28, 2004** | **Lightweight_BoF.pl** | **Proof of Concept exploit script for the Lightweight FTP Server Remote Buffer Overflow vulnerability.** |
| May 28, 2004 | WifiScanner-0.9.4.tar.gz | An analyzer and detector of 802.11b stations and access points that listens alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz. |
| May 27, 2004 | metaexpl.tgz | Remote exploit script for the Metamail buffer overflow vulnerability. |
| **May 27, 2004** | **phpInputWrapperIncludeExploit.php** | **Script that exploits the PHP 'include()' function Remote Command Execution vulnerability.** |
| May 26, 2004 | bash-perassi.patch | A patch for bash that modifies the shell to send all user keystrokes via UDP over the network for collection by a sniffer or a syslogd server. |
| May 26, 2004 | publimark-0.1.1.tgz | A command line tool that secretly embeds text in an audio file. |
| May 26, 2004 | rkhunter-1.0.9.tar.gz | Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers. |
| May 25, 2004 | Orenosv-Dos.c | Script that exploits the Orenosv HTTP/FTP Server Remote Denial of Service vulnerability. |
| May 24, 2004 | cvs_solaris_HEAP.c | Script that exploits the CVS Buffer Overflow vulnerability. |
| May 24, 2004 | killvoc-small.c | Script that exploits the VGW120/ VGW480 Telephony Gateway Remote H.225 Denial Of Service vulnerability. |

# ***Trends***

- **US-CERT has received reports of scanning activity directed at port 5000/tcp. This port is used by the Microsoft Windows Universal Plug and Play service (UPnP). There are known vulnerabilities in UPnP, for which a patch has been available (Microsoft Security Bulletin MS01-059).**
- **US-CERT has received reports of a new worm, referred to as "W32/Sasser". This worm attempts to take advantage of a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). See Microsoft Security Bulletin located at: http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx. The vulnerability allows a remote malicious user to execute arbitrary code with SYSTEM privileges. There are several variants of this worm circulating in the wild. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **Fraudulent e-mails designed to dupe Internet users out of their credit card details or bank information topped the three billion mark last month, according to one of the largest spam e-mail filtering companies. The authentic-looking e-mails, masquerading as messages from banks or online retailers, have become a popular new tool for tech-savvy fraudsters in a new scam known as "phishing".**

## Viruses/Trojans

Viruses and Trojans have become increasingly popular as means of obtaining unauthorized access to computer systems. The following table encompass new viruses, variations of previously encountered viruses, and Trojans that have been discovered in the last two weeks. They are listed alphabetically by their name. While these viruses and Trojans might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. Readers should also contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Following this table are write-ups of new viruses and Trojans that are considered to be a high level threat. *NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.*

*The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.*

| Name | Aliases | Type |
|---|---|---|
| Backdoor.Ducy | | Trojan |
| Backdoor.IRC.Aladinz.R | | Trojan |
| Backdoor.Mtron | IRC-Mtron | Trojan |
| Backdoor.Nibu.G | | Trojan |
| BAT.Sebak | | Trojan |
| Downloader-KP | | Trojan |
| IRC/Krisworm-C | | mIRC or pIRCH Script Worm |
| IRC-Scanbot | | Trojan |
| JS.Offiz | Trojan.JS.Offiz<br>JS/Offiz | Trojan |
| OF97/Exedrop-C | | Office 97 Macro Virus |
| Reboot-AF | | Trojan |
| StartPage-BQ | | Trojan |
| StartPage-DA | | Trojan |
| StartPage-DC | | Trojan |
| StartPage-DL | | Trojan |
| Troj/Agent-A | TrojanDownloader.BMP.Agent.a<br>Exploit-BMP.dldr | Trojan |
| Troj/Dloader-IU | | Trojan |
| Troj/Inor-I | | Trojan |
| Troj/Iyus-A | PWSteal.Trojan | Trojan |
| Troj/Orifice-G | Backdoor.BO2K.n<br>Orifice2K trojan<br>BO2K.Trojan Variant | Trojan |
| Troj/Sdbot-BI | Backdoor.SdBot.kd<br>W32/Spybot.worm.gen.b<br>Win32/SpyBot.WW<br>Backdoor.IRC.Bot | Trojan |
| Troj/StartPa-AE | Trojan.WinREG.StartPage | Trojan |
| Trojan Notifier | TrojanNotifier | Trojan |
| Trojan.Bookmarker.I | TROJ_KREPPER.E | Trojan |
| Trojan.Delrun | Trojan.JS.Zxdow<br>VBS/Winrun, VBS_ZIKDOW.GEN | Trojan |
| Trojan.Dingsta.A | TROJ_ASTUX.A<br>Keylog-Dingxa | Trojan |

| Name | Aliases | Type |
|---|---|---|
| Trojan.Gema.B | Downloader.Crypter.E<br>TrojanDownloader.Win32.Crypter<br>Trojan.Crypter.C<br>Trojan.DownLoader.36864<br>W32/Crypter.A, SysCenter<br>Trojan.Downloader.Win32.Crypter,<br>Win32/TrojanDownloader.Crypter.A<br>Troj/Crypter-C<br>TrojanDownloader.Crypter | Trojan |
| Trojan.Mitglieder.L | TrojanProxy.Win32.Mitglieder.bi | Trojan |
| Trojan.Startpage.E | | Trojan |
| VBS.Krim.G@mm | VBS/Rimko@mm | Visual Basic Script Worm |
| VBS.Nevesc | VBS.Neves<br>VBS.Pookins | Visual Basic Script Worm |
| VBS.Powcox@mm | I-Worm.Powcox.a<br>VBS/SevenC | Visual Basic Script Worm |
| VBS.Pub | | Visual Basic Script Worm |
| VBS.Startpage.C | Trojan.StartPage.C | Trojan |
| VBS.Yeno@mm | VBS.Entice | Visual Basic Script Worm |
| W32.Antinny.Q | | Win32 Worm |
| W32.Bugbear.G@mm | | Win32 Worm |
| W32.Dabber.B | | Win32 Worm |
| W32.Donk.R | | Win32 Worm |
| W32.Explet.A@mm | | Win32 Worm |
| W32.Gaobot.ALU | | Win32 Worm |
| W32.Gaobot.ALV | | Win32 Worm |
| W32.Gaobot.ALW | | Win32 Worm |
| W32.Gaobot.AOL | | Win32 Worm |
| W32.Gaobot.FO | Backdoor.Agobot.3.gen<br>W32/Gaobot.worm.gen.d | Win32 Worm |
| W32.Gaobot.RB | W32/Gaobot.worm.gen.e | Win32 Worm |
| W32.Joot.A@mm | | Win32 Worm |
| W32.Kibuv.C | | Win32 Worm |
| W32.Kibuv.D | | Win32 Worm |
| W32.Kibuv.E | | Win32 Worm |
| W32.Korgo.I | | Win32Worm |
| W32.Netsup.A@mm | | Win32 Worm |
| W32.Rainwash | | Win32 Worm |
| W32.Shoes@mm | | Win32 Worm |
| W32.Svoy.A@mm | I-Worm.Svoy.a<br>W32/Svoy.worm.gen | Win32 Worm |
| W32/Agobot-JA | Backdoor.Agobot.mw<br>W32/Gaobot.worm.gen.e<br>Win32/Agobot.3.T<br>W32.HLLW.Gaobot.gen<br>WORM_AGOBOT.MW | Win32 Worm |
| W32/Agobot-JB | Gaobot<br>Nortonbot<br>Phatbot<br>Polybot | Win32 Worm |
| W32/Agobot-JF | Gaobot<br>Nortonbot<br>Phatbot<br>Polybot | Win32 Worm |

| Name | Aliases | Type |
|---|---|---|
| W32/Agobot-JM | Backdoor.Agobot.gen<br>W32/Gaobot.worm.gen.d<br>W32.HLLW.Gaobot.gen | Win32 Worm |
| W32/Agobot-SG | | Win32 Worm |
| W32/Agobot-XX | | Win32 Worm |
| W32/Francette-K | Worm.Win32.Francette.l<br>W32/Tumbi.worm.gen.b<br>W32.Francette.Worm<br>WORM_FRANCETTE.L | Win32 Worm |
| W32/Parparo.worm | HLLP.Scrambler.B | Win32 Worm |
| W32/Rbot-T | Backdoor.Rbot.gen<br>W32/Sdbot.worm.gen.h | Win32 Worm |
| W32/Rbot-V | Backdoor.Spyboter.bx<br>W32/Sdbot.worm.gen.i<br>Win32/Spyboter.BX<br>W32.Randex.gen<br>WORM_SDBOT.JT | Win32 Worm |
| W32/Rbot-X | | Win32 Worm |
| W32/Rbot-Y | Backdoor.Rbot.b<br>W32.Spybot.Worm | Win32 Worm |
| W32/SdBot-BC | INFECTED Backdoor.Rbot.gen<br>W32/Sdbot.worm.gen.m<br>W32.Spybot.Worm | Win32 Worm |
| W32/Sdbot-BW | Backdoor.SdBot.ma | Win32 Worm |
| W32/Sdbot-DB | | Win32 Worm |
| W32/Spybot-BZ | | Win32 Worm |
| W32/Spybot-CC | | Win32 Worm |
| W32/Spybot-CG | Spybot.worm.gen.e | Win32 Worm |
| W64_RUGRAT.A | W64.rugrat.3344<br>W64/Rugrat | File Infector |
| W97M.Asmah.A | | Word 97 Macro Virus |
| W97M.Nobody | | Word 97 Macro Virus |
| Worm/Agobot.300544 | Worm.Agobot.SU | Internet Worm |
| Worm/Rbot.94208 | Win32.Rbot | Win32 Worm |
| WORM_AGOBOT.GN | | Internet Worm |
| WORM_AGOBOT.SU | | Internet Worm |
| WORM_ANIG.A | W32/Dfcsvc.worm<br>W32/HLLW.Anig | Win32 Worm |
| WORM_KORGO.A | W32.Korgo.A<br>Worm.Win32.Padobot.b<br>Exploit-Lsass.gen | Win32 Worm |
| WORM_KORGO.B | W32.Korgo.B<br>Worm.Win32.Padobot.a | Win32 Worm |
| WORM_KORGO.C | | Win32 Worm |
| WORM_KORGO.D | W32.Korgo.D<br>Worm.Win32.Padobot.Gen | Win32 Worm |
| WORM_KORGO.E | W32.Korgo.E | Internet Worm |
| WORM_KORGO.F | W32.Korgo.F<br>Worm.Win32.Padobot.e<br>W32/Korgo.worm.g | Internet Worm |
| WORM_KORGO.G | W32.Korgo.G | Internet Worm |
| WORM_KORGO.H | W32.Korgo.H | Internet Worm |
| WORM_LAMUD.A | | Win32 Worm |

| Name | Aliases | Type |
|---|---|---|
| WORM_PLEXUS.A | I-Worm.Plexus.a<br>W32.Explet.A@mm<br>W32/Plexus@MM<br>W32/Dumaru-AK<br>TrojanDropper.Win32.Mudrop.h<br>W32/Plexus@MM virus<br>Worm.Win32.Plexus.a | Internet Worm |
| WORM_PLEXUS.C | Win32/Plexus.B@mm<br>I-Worm.Plexus.b | Win32 Worm |
| WORM_RANDEX.AK | | Win32 Worm |
| WORM_SDBOT.MG | W32/Randex.Z<br>Backdoor.Rbot.gen | Win32 Worm |
| Zerolin | TrojanDropper.VBS.Zerolin<br>VBS/Zerolin | Trojan |

**W32/Korgo.F:** US-CERT has received reports of a new worm, referred to as "W32/Korgo.F" or "W32/Padobot". This worm attempts to take advantage of a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). The vulnerability allows a remote malicious user to execute arbitrary code with SYSTEM privileges. More information on this vulnerability is available in Vulnerability Note VU#753212 and Microsoft Security Bulletin MS04-011. The worm propagates by scanning random IP addresses on port 445/tcp for vulnerable systems. Upon finding a vulnerable system, the worm will attempt to exploit this vulnerability. If successful, this worm will open a connection on port 113/tcp or port 3067/tcp and may attempt to connect to a list of pre-determined IRC servers. US-CERT strongly encourages users to install and maintain anti-virus software as well as patch their systems to prevent exploitation of this vulnerability.